Interoperation Key Schema for Social Media Tools in IP Multimedia Subsystem

R. Muthaiah[1], B. D. Deebak[1], K. Thenmozhi[2], and P. Swaminathan[1]
[1]School of Computing, SASTRA University, Thanjavur-613401, INDIA
[2]School of Electrical and Electronics, SASTRA University, Thanjavur-613401, INDIA
Email: sjamuthaiah@core.sastra.edu jrvd_deebak@ymail.com deanpsw@sastra.edu
thenmozhik@ece.sastra.edu

Abstract— IP Multimedia Subsystem (IMS) is now being a solution for packet switched networks. The future generation network is amalgamating the infrastructure of Wireless / wire-line for providing the standard interface for Internet services. Nevertheless, the network infrastructures like multimedia and non-multimedia do not have any native mechanism to interpret the key schema of client media tools to establish the communication such as voice and data. To establish, as such services, a signaling protocol of Session Initiation Protocol (SIP) is being put to use to control the communication on Internet for establishing, Maintaining and terminating the communication session. Many papers have been proposed for authentication and authorization for securing the communication media. However, so far, no paper has been proposed for interpreting the built-in schema of multimedia tools. Thus we propose the Interoperation Key Schema to successfully exchange the mismatched schema between media client and server. Also we analyze the proposed mechanism with Internet security systems of Internet Protocol Security (IPSec) and Transport Layer Security (TLS). We deploy a real time platform of multimedia to examine the interoperation success rate and call setup time between the media clients.

Index Terms—IP multimedia subsystem, session initiation protocol, internet protocol security and transport layer security

I. Introduction

The aim of future generation network is to amalgamate the communication paradigm of Internet and cellular networks. To provide ubiquitous services to the above paradigm, Third Generation (3G) network has found the key element of IMS. To access the services of multimedia, the handheld devices of multimedia need to be enabled in 3G network. When the multimedia network service is found and configured with the device, then the subscriber could be able to access the services like web chatting, internet telephony, instant messaging, voice call and video conference call.

A. Background

An Architecture of Universal Mobile Telecommunication System (UMTS) defines the IMS services. Moreover, the UMTS divides the multimedia services as voice and data. Third Generation Partnership Project (3GPP) [1] has named the IMS as networking subsystem. 3GPP standardizes the architecture of IMS.

The first release of 3GPP was named as Release 99 (R99) and it was released in 1999. The R99 was comprised of general system architecture, core network services and network standard interfaces such as Time Division Code Division Multiple Access (TD-CDMA), Wideband Code Division Multiple Access (W-CDMA) and Frequency Division Code Division Multiple Access (FD-CDMA) [2]. IP based multiple access network has been contrived since the release of R99. The architecture of IMS was too complex. Hence the 3GPP divided the development work as Release 4 (R4) [3] and Release 5 (R5) [4]. R4 was issued in 2001 and it was focused on the specification of Internet transport networks. The IMS was focused on the release of R5 and it was completed in 2002. The functional services of IMS were stabilized in the Release6 (R6) [5]. The core components of IMS were adopted with Fixed Mobile Convergence (FMC) in 2007 as Release 7(R7) [6].

IMS services are delivered through the IP transport layer. The IP transport layer is also known as Session Initiation Protocol (SIP) [7]. Internet Engineering Task Force (IETF) was designed this signaling protocol and it was standardized as RFC 3261. The aim of the signaling protocol is to establish, maintain and terminate the established session between the parties. Moreover, it is designed and developed to be an independent protocol; thus it does not over-rely on the transport layer. The data streaming protocols such as Real Time Transport Protocol (RTP) and Real Time Streaming Protocol (RTSP) uses to control the media session that is between the end users.

Recently, the researchers have had an enormous paper on an authentication schema for securing the SIP communication [8]-[14].

SIP can't provide stronger security mechanism; therefore the mechanism of HTTP digest authentication is proven to be insecure [15]. Since the schema of HTTP digest is based on the original SIP authentication schema, it can exploit by the vulnerabilities of offline password guessing attack and server spoofing attack [14]. The schema of Diffie-Hellmann key exchange [16] is not suitable for low power consumption, owing to, high

Manuscript received June 12, 2013; revised October 28, 2013.
This work is supported by the TATA Consultancy Services (TCS) under the scheme of Research Scholar Program (RPS)
Corresponding author email: sjamuthaiah@core.sastra.edu.
doi:10.12720/jcm.8.11.730-737

computational cost. In the cause of improvement, the approach of Elliptic Curve Diffie-Hellman was proposed in 2007 [17]. Authorization and Authentication have been a challenging task of IMS environment [18]-[21]. The key schemas have been introduced for securing the media communication [22]-[23]. Since the schema of Tsai's is not providing the known-key and perfect-forward secrecy, it could still be exploited by the vulnerabilities of password guessing and stolen-verifier attack [24].

Multimedia User Equipment (M-UE) employs the Authentication and Key Agreement (AKA) protocol to secure the multimedia sessions. Many research studies [25]-[31] have been done for AKA, but then, most of the existing techniques of AKA are not suitable for wireless mobile communication networks. It is owing to power constraints, bandwidth utilization and user authentication. So far none of the researchers have drawn out an idea for client interoperation (different UE communication) and authentication schema exchange. In [32], [33], the authors propose a technique of public key crptosystem-Elliptic Curve Cryptography (ECC) and its feature is ECC which has the parameter of per-key-bit to strengthen the session key.

The Authentication schemas such as IMS-AKAV1 an IMS-AKAV2 analyzes the security issues of IP Telephony well rather than the key interoperation. It uses the parameters like RAND and AUTH to specify the nounce parameters. It is failing to prevent the 'Interleaving Attack', because, it uses the different context for same credentials. Importantly, it does not have any proactive steps to interoperate the key schema while the communications are being progressed. The communications are thereby terminated / tampered by the anonymous users. To overcome this issue, an IMS-AKAV2 proposed to prevent the man-in-the-middle attack. But then, it does not have a strategy of key interoperation to prevent the unnecessary events like call termination, key exchange and anomalous deduction while the service being progressed.

The schemas like HTTP-Digest, Diffie-Hellmann key exchange and Elliptic Curve Diffie-Hellman and Tsai's also discuss the security mechanism, though the mechanism does not have the interoperation mechanism. Thus this research article confidently states that so far of the research papers on the topic of key schemas have not had an interoperation technique to exchange the mismatched schema for authorized users. So, this research paper focuses on to resolve such issues by the technique of Interoperation Key Schema (IKS).

This schema is run along with media server with IMS Core to investigate the metrics of interoperation success rate and call setup time. The media clients such as X-lite [34] and Zoiper [35] are used to be acted as the media end-users. The authentication Schema of IMSCore and Clients are redesigned and redeveloped in the Linux and Windows platform to evaluate the voice service.

B. Research Contribution

The contributions of this paper are precisely abstracted that are as follows.

1) We design and develop Interoperation Key Schema for media clients. This schema does the interoperation while the client schemas are mismatched
2) We incorporate this novel schema in the IMSCore environment to investigate the communication of media clients in heterogeneous networks. This schema does the following communication efficiently 1) Heterogeneous Multimedia Communication (Lnux OS to Windows OS)
3) We run the IMSCore [36] environment in the Linux platform to establish the communication for multimedia clients (that X-Lite [34] and Zoiper [35]). The novel mechanism of IKS integrates with IMSCore to examine the service of voice call
4) We also integrate the IMSCore environment with Ntop [37] (A traffic analysis tool) to analyze interoperation success rate and call setup time
5) The proposed mechanism of IKS compares with the existing mechanism of IMS-AKA1, IMS-AKA2 and MD5. Moreover, the mechanisms will be compared with IMSCore environment.

C. Related Work

3GPP standardizes the IMS and it is commonly known as Internet Protocol (IP) Based Overlay Networks. Though the specifications of IMS focus on the UMTS and General Packet Radio Service (GPRS), its concepts is to access the networks independently. The current specification of IMS considers the Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (WiMAX) and Fixed Mobile Convergence (FMC) as an IMS network access region to provide secure end-to-end Quality of Service (QoS) to the customers. However, it could not offer the client interoperation. Signaling of IMS is IP based and it has two well-known interfacing protocols of Internet Engineering Task Force (IETF): SIP [32] and Diameter Peer [33]. The enhancement of these protocols is to fulfil the requirements of the IMS. Thus an extensive research study has been made in resolving the issue of interoperation and media session maintenance. This section portrays the functional components of IMS core, authentication schema of IMS, deployment challenges of IMS and media traffic in IMS.

IMS network hosts the signal operation to collaborate easily with the foreign access networks using the dedicated mechanism. The purpose of the mechanism is to attain the protocol compatibility and enforce the Quality of Services (QoS) with seamless mobility. IMS realizes the network versatility and authentication schemes to deliver the user information to serve the services of multimedia such as voice / video. IMS encompasses of signaling server components and data storage. The server components are generally called as Call Session Control Function (CSCF) and they are used

to handle the user data calls. CSCF does the following tasks. Task1 is to ensure the translation and routing of calls. Task2 is to integrate the management of QoS. Task3 is to configure the function of media transcoding. Task4 is to integrate the services with user profile to access the communication privileges.

The components of CSCF's are

Proxy-Call Session Control Function (P-CSCF) – it locates at the network border of IMS and it uses the infrastructure of packet switched network to route the data call to the appropriate P-CSCF which resides at the other side of the IMS networks. It does the service translation and routing through the Serving-Call Session Control Function (S-CSCF).

Serving Call Session Control Function (S-CSCF) – it accepts the call request which is translated by the P-CSCF. It checks the user identity, privileges and schema matches with the database of IMS networks to serve the requested service.

Interrogating – Call Session Control Function – it interoperates the clients to collaborate with networks of foreign IMS. It interchanges the user profile, service privilege and charging system to the roaming network.

Besides IMS uses the Home Subscriber Server (HSS) to relate the user data such as user profile, privileges, charging system and configuration data of Application Server (AS) to host the services of the user. A signaling protocol of Session Initiation Protocol (SIP) is adopted to manage the services of IMS in IP networks. This protocol hosts the operations like session establishment, maintenance and termination. In contradict to H.323 protocol of International Telecommunication Union (ITU); this signaling protocol has message format extensibility and ease integration of fields and types. IMS is incorporated with multiple access networks to access the various network interfaces.

TABLE I. NOTATIONS

AV	Authentication Vector
MAR	Multimedia Authentication Request
MAA	Multimedia Authentication Answer
AUTN	Authentication Token
SAR	Server Authentication Request
SAA	Server Authentication Answer
UE^i	User Equiment
RAND	Random Value of i^{th} Integer
Public Key	$K_{pub}{}^{i}{}_{1}$ and $K_{pub}{}^{i}{}_{2}$
Interoperation Key	I_{s1} and I_{s2}
r	Random Number
⊕	Ex-Or Operator
Private Key	P
Sig^i_1	Signature of i^{th} Key
p	Prime Number
q	Order
Public Key	P_{pub1} and P_{pub2}
Public Key (After Interoperation)	$K_{pub}{}^{i}{}_{1}$ and $K_{pub}{}^{i}{}_{2}$
Private Key (After Interoperation)	$K_{pv}{}^{i}{}_{1}$ and $K_{pv}{}^{i}{}_{2}$
h( )	One Way Hash Function
Ğ1,Ğ2	Cyclic Group
Ĕ	Order

The forthcoming sections are devised as follows. Section II recounts the Interoperation Key Schema for IMS. Section III divulges the experimental analysis of multimedia server-client setup and schema analysis. Section IV concludes this research paper.

II. REVIEW ON INTERCONNECTION SCHEMES OF SIP

The architecture of IMS cooperates with a packet switching network and such cooperativeness has brought the numerous logical interfaces. The SIP protocol manifests the implementation of logical interfaces. The feature of flexibility is provided to SIP to build up the message structure of Session Description Protocol (SDP) [38]. The structured format of an SDP permits the new definition of massage, a new association of parameters and new options for not affecting the existing procedures. Third Generation Partnership Project (3GPP) [39] standardizes the logical interfaces and it forms the topologies to interconnect the access networks with IMSCore.

The interface of Gm [39] uses to configure the SIP protocol between IMSCore and multimedia applications. Such interface configuration does the following functional performance as it is shown in Fig. 1.

1) It discovers the server of Proxy Call Session Control Function (P-CSCF) to route the data calls.
2) It discovers the server of Serving Call Session Control Function (S-CSCF) to inspect the user identity, privileges, schema exchange and service charging records.
3) It discovers the server of Interrogating Call Session Control Function (I-CSCF) to perform the network interoperation, user profile exchange, access privilege and roaming service charges.

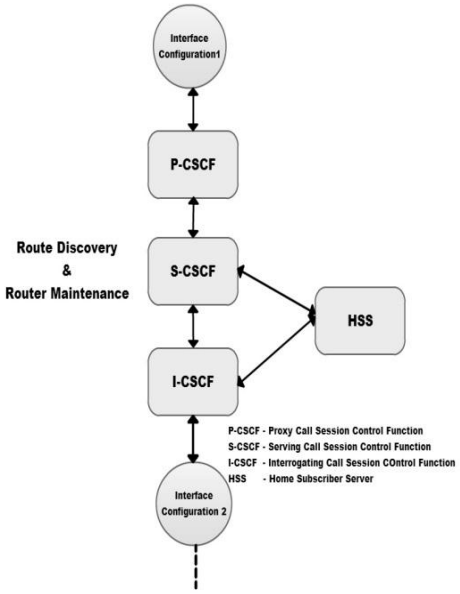

Figure 1. Functional performance of IMS

4) It discovers the server of Home Subscriber Server (HSS) to authenticate and authorize the multimedia users of IMSCore.

The interface of M_w defines two versions. First version is Network-To-Network Interface (NNI) and the second version is User-To-Network Interface (UNI). Moreover, the first version is used to handle the user data through IMSCore network and the second version is used to transfer the communication between S-CSCF and P-CSCF. The communication is transferred in the same IMSCore. The interface of C_x communicates with Application Server (AS) to interpret the user credentials with Home Subscriber Server (HSS) through the S-CSCF. The interface of IMS Service Control Interface (ISC) is used to translate the notification message between the AS and S-CSCF. The interface of Sh uses the AS to communicate with HSS. The interface of G_m is exploited to get connected with IMSCore. The interface of Z_b is used to allow the basic configuration of the module. The interface of Za is used to interface the network entities and Security Gateway (SEG). Z_a interfaces different security domain whereas Z_b interfaces the same network entity and security domain. Fig. 2 illustrates the network domain interfaces of IMS.

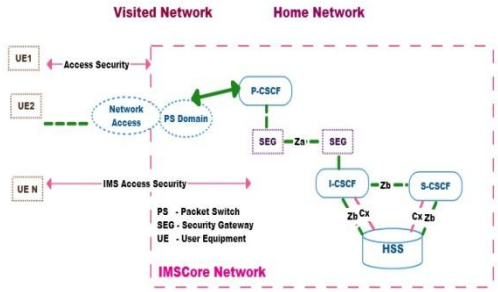

Figure 2. Network domain interfaces of IMS

IMS Core is not harmonized properly with IMSCore for exploiting the user resource allocation mechanism.

The allocation mechanism is done to setup a dedicated data encapsulation. The class of QoS offers a generic binding scheme to bind the resource of access network. IMSCore should setup the streaming protocol of RTP with the precise requirement of QoS. This is a complicated procedure for multiple access networks. Thus a novel technique of forward and backward seeker strategies has been proposed for mitigating the congestion rate of IP based heterogeneous multiple access networks.

This novel mechanism has signaling and oscillation indexes to enforce the IMS signal control on the backbone of the IP heterogeneous infrastructure to introduce the signal congestion control mechanism and signal call admission control. This mechanism amalgamates

1) Monitored the network signals for negotiating the rate of congestion which helps to improve the usage of bandwidth and network performances.
2) Seeker mechanism helps to mitigate the end-to-end response delay of the voice call and enhance the call success delivery ratio. The forthcoming section elaborates the mathematical strategies of forward and backward seeker to mitigate the rate of congestion on the IP based access network. References

A. Authentication Protocol of IMS-AKA

(Version 1 and 2)

Number Presume that the Multimedia Users (MU's) are authenticated strongly at the PS domain. SIP register requests and responses are used to process the protocol of IMS-AKA. The phase 1 of communication flows is discussed henceforth.

F1: Through I-CSCF and P-CSCF, the MU traverses the SIP request to the S-CSCF.

F2: IF the MU and S-CSCF Authentication Vectors (AV's) are not matched then the S-CSCF communicates the HSS over C_x interface by the request method of Multimedia Authentication Request (MAR) to obtain the AV. Else this step and next step could be skipped.

F3: AV's are generated as an ordered array by HSS. The ordered array will be then traversed to the S-CSCF over C_x interface via Multimedia Authentication Answer (MAA).

F4: S-CSCF utilizes the Unused Authentication Vector (AV) from the ordered array to validate UE through SIP 401 unauthorized message.

F5: UE evaluates the generated AUTN. If it is positive then UE computes the RES, C_k and I_k. The computed RES will be then forwarded to the S-CSCF through P-CSCF and I-CSCF.

F6: S-CSCF evaluates the user response of XRES and if the evaluation shows the positive then the authentication keys will be exchanged. Else the Server Authentication Request (SAR) is traversed over C_x interface to inform HSS that S-CSCF serves the UE

F7: The user profile and S-CSCF name are stored with HSS over C_x interface through Server Assignment Answer (SAA)

F8: Eventually, a message of SIP 200Ok sends to UE to notify the successful registration through S-CSCF

The phases 2 of communication flows are to secure the P-CSCF and UE. The P-CSCF and UE are secured during the completion of Phase 1 through the field of Secure Client and Server. The AV's are secured through the field of Secure Computation to hold on with Man-In-The-Middle attack. The existing schemes like IMS – AKAV1 and IMS-AKAV2 were successfully integrated with the IMSCore networks. The schemes are also integrated with the clients like X-lite and Zoiper to examine the schema interoperability.

III. Proposed Schema of IKS

This section describes the novel mechanism of IKS for IMS. This generates the interoperation authentication vector using the mechanism of IMS-AKA1, AKA2 and MD-5. The objective is to interoperate the authentication vectors through the mechanism of IKS. This mechanism proves to be a best to interoperate the different IMS and non-IMS clients. HSS is integrated with IMSCore to

compute the interoperation AV's and the interoperated AV's are shared in between the multimedia clients to establish the media sessions.

The HSS has a server of IMSCore that generates the interoperation key vector for the UE. We presume the bilinear map $\check{E}: \check{G}1 * \check{G}1 \rightarrow \check{G}2$. The IMSCore randomly chooses the interoperation key $I_{s1}. I_{s2}, I_{s3}, \ldots\ldots \in Z^*_q$ as the two master keys as to compute the public keys of $P_{pub1} = I_{s1}$ and $P_{pub2} = I_{s2}$. In this work, we presume that the UE has two interoperation shared key (I_{s1} and I_{s2}). IMSCore parameters are order (q), prime number (p), private number (P), Public Keys (P_{pub1} and P_{pub2}) and Map To Point function.

The proposed solutions are discussed as follows.

S1: UE^i starts communicate with different multimedia clients by the use of interoperation shared key.

S2: UE^i traverses the SIP request by the inclusion of private and public key to share the interoperation key while different platform/media clients get into communication.

1) Public Key $Kpub^i_1$ and $KPub^i_2$ to generate the interoperation key from the IMSCore

$$Kpub^i_1 = r.P \text{ and } KPub^i_2 = \grave{U}\check{E}\bar{I}\check{D} \oplus h(r.P_{pub1}) \quad (1)$$

2) Where r is a random number and $\oplus$ is an XOR operator
3) Interoperation Key Vector will have $RAND^i$ to compute the share interoperation key
4) The private key Kpv^i_1 and Kpv^i_2 are to encrypt the share interoperation key

$$Kpv^i_1 = I_{s1} . K_{pub}{}^i_1 \text{ and } Kpv^i_2 = I_{s2} . h(K_{pub}{}^i_1 \,||\, K_{pub}{}^i_2 \quad (2)$$

S3: In the event of connection establishment, the generated interoperation keys should be shared in parallel to receive the SIP message of '401 Unauthorized'

S4: Using the private keys ($K_{pv}{}^i_1$ and $K_{pv}{}^i_2$), the UE^i extracts the interoperation keys. It uses to compute the signature

$$Sig^i_1 = K_{pv}{}^i_1 + h(RAND^i).K_{pv}{}^i_2 \quad (3)$$

The UE^i validates the $K_{pub}{}^i_1$ and $K_{pub}{}^i_2$ using the model of

$$\check{E}(Sig^i_1, P) = \check{E}(K_{pv}{}^i_1 + h(RAND^i).K_{pv}{}^i_2, P) \quad (4)$$

$$= \check{E}(K_{pv}{}^i_1, P) . \check{E}(h(RAND^i).K_{pv}{}^i_2, P)$$

$$= \check{E}(K_{pub}{}^i_1, P) . \check{E}(h(RAND^i).I_{s2}. h(K_{pub}{}^i_1 || K_{pub}{}^i_2), P)$$

$$= \check{E}(K_{pub}{}^i_1, P) . \check{E}(h(RAND^i). h(K_{pub}{}^i_1 || K_{pub}{}^i_2), I_{s2}, P)$$

$$= \check{E}(K_{pub}{}^i_1, K_{pub}{}^i_2) . \check{E}(h(RAND^i). h(K_{pub}{}^i_1 || K_{pub}{}^i_2), P_{pub2})$$

S5: When the interoperation keys are shared, the services like voice, video and data could be availed not only for same multimedia clients but also for different multimedia clients.

A. Advantage of IKS

This mechanism has the following the merits for the IMSCore environment.

1) This can reduce the generation and verification delay. It does the reduction particularly in a large number of signatures.
2) It does not use AKAV1-MD2 and AKAV2-MD5. Therefore the incorporated model provides the code simplicity. It does not consume much memory to generate the interoperation keys. Moreover, it does the key computation rapidly reduce the latency.
3) This mechanism is based on hybrid cryptography. Thus it needs to have mutual authentication between the IMSCore and IMSClient. The former can't have a feature of key retrieval; therefore we should have a proper encryption mechanism to guarantee the secure communication.

IV. Experimental Analysis

This section describes the analysis of IKS and its session interoperation strategy. We investigate the proposed scheme of IKS with IMS core and multimedia clients (X-lite[34] and Zoiper[35]) to probe 1. Interoperation Success Rate 2. Call Setup Time. In [40], [41], the author's design and develop a model of real time IMS environment to analyze the signaling efficiency. In lieu of that, an environment of the IMS core platform and clients (Linux and Window Supporting Clients) are redesigned and redeveloped to proficiently testify the proposed schemas of IKS like 1. IMSCore with IKS 2. IMSCore with AKAV1-MD5 3. IMSCore with AKAV2-MD5. A voice call is one of the best effort mode of service for the client's communication. Thus, it is chosen to validate the proposed schemas of this paper. Fig. 3 illustrates Real Time IMS Domain Environment.

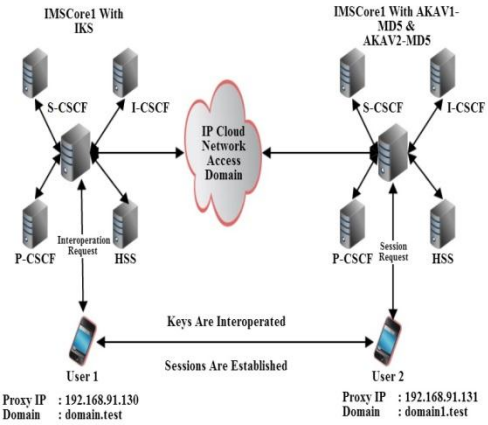

Figure 3. Network domain interfaces of IMS

Fig. 3 choose the heterogeneous network to investigate the schemas of IKS and its associated interoperation strategy. We redeploy and reconfigure the IMSCore in two different Linux platforms as to have domain of cloud IP. The first domain of IMS is called as IMSCore1 with IKS and it is deployed and configured in Linux Mint (Version 14). The server IP of this domain is set as '192.168.91.130' and realm of this domain is set as 'domain.test'. It has three call session control functions

(Proxy, Serving and Interrogating) and one user authentication server (Home Subscriber Server). It is integrated of ASI to check the network usage, to prevent the session blocks in the media channel and to retain the usage of the network as below of 4.5%.

Eventually, it has the IMS client (whose public identity is sip: alice@domain.test) and its schema is successfully interoperated with IMSCore1 with IKS to have a session with the client of IMSCore2 with AKAV1-MD5 and AKAV2-MD5.

The second domain of IMS is called as IMSCore2 with AKAV1 and V2 – MD5 and it is deployed and configured in Ubuntu Desktop (Version 12). The server IP of this domain is set as '192.168.91.131' and realm of this domain is set as 'sastratcs.test1'. It has three call session control functions (Proxy, Serving and Interrogating) and one user authentication server (Home Subscriber Server). It is integrated of AKAV1-MD5 and AKAV2-MD5 to check the network usage, to prevent the session blocks in the media channel and to retain the usage of the network as below of 4.5%. Eventually, it has the IMS client (whose public identity is sip:bob@domain.test1) and its schema is successfully interoperated with IMSCore2 with (AKAV1 and V2 – MD5) to have a session with client of IMSCore1 with IKS. A real traffic analyzer tools Ntop [37] is integrated with IMSCore domain to monitor the call response time of clients.

A. Heterogeneous Multimedia Communication (Linux To Windows IMS Clients)

We successfully configure the IMS Core1 with IKS, IMSCore2 with AKAV1-MD5 and IMSCore2 with AKAV2-MD5 in the Linux Operating Systems (Linux Mint and Ubuntu) to testify the heterogeneous multimedia communication.

Step1: We choose the X-Lite [34] as a Linux IMS client

Step2: We successfully configure and execute the SIP client in the Linux Mint OS

Step3: The schema of client interoperates with IMS Core1 with IKS

Step4: We choose the Zoiper [35] as Windows IMS client

Step5: The schema of client interoperates with IMS Core2 with IKS

Step6: We distinguish the results as IMS Core1with IKS, IMSCore2 with AKAV1-MD5 and IMSCore2 with AKAV2-MD5.

We run IMS Core1 with IKS in the Linux Mint OS and we run IMS Core2 (AKAV1-MD5 and AKAV2-MD5) in the Ubuntu Desktop OS as well in parallel to serve the service of voice call service to multimedia clients. We patch the IKS with IMS Core 1 to interpret the client's schema to establish the service session.

We employ IMSCore1 and IMSCore2 as the Testbed of Multimedia Networking. We employ X-lite[34] and Zoiper [35] as the Testing Clients of Multimedia. We install the X-Lite in Linux Mint OS and the Zoiper in Windows 7 OS. The authorized user of 'Alice' is registered in the X-lite of IMSCore 1 and the authorized user of 'Bob' is registered in the Zoiper of IMSCore 2. We configure 100 Base T_x Switch to interconnect the PC's Ethernet hubs.

TABLE II. CONFIGURATION SETUP OF IMSCORE (1 AND 2)4

Internal Parameters	Setup Values
IMSCore (1&2) Execution Time	1 Hrs
Voice Call Time	1 Hrs
Supporting Codec	VLC, PCMU and PCMA
Packet Discard Ratio	0.02%
Packet Transfer Latency	Exponential of 0.05 Sec
Call Rsponse Time	2 ms
Bandwidth Range	1 – 100 Mbps
Access Network	IEEE 802.11b
IPSec	Enabled
TLS	Enabled

Table II illustrates the Real Time Configuration Setup of IMS Core (1&2). This illustration reveals Execution Time of IMS Platform (in hrs), Voice Call Duration Time (in hrs), Voice Codec, Packet Discard Ratio (in ms), Packet Transfer Latency (in ms), Call Response Time (in ms) and Bandwidth Range (in Mbps). For research analysis, the IMS Core runs for one hour. For media session analysis, the voice call establishes between the clients for an hour.

X-Lite [34] supports BroadVoice-32 and G711 from the released version of 2012 and Zoiper supports the audio codec such as PCMU, PCMA and MPA.

TABLE III. INTEROPERATION SUCCESS RATE (%)

Protocols	Minimum	Maximum	Average
AKAV1-MD5	22.2	43.2	31.7
AKAV2-MD5	22.9	54.2	31.4
Proposed IKS	88.7	98.8	94.7

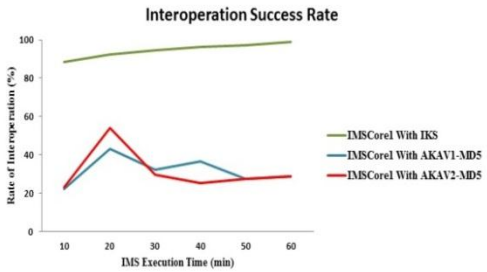

Figure 4. Interoperation success rate

Fig. 4 illustrates interoperation success rate. We deploy and configure the multimedia clients with 12PC's to interrogate the schema success rate. We test the success rate of interoperation using Ntop[37] and Wireshark [42]. The result shows in Table III wherein IMS Core with IKS does the schema interoperation at on-time to serve the requested multimedia service (the opted service is voice call). We probe the IMS environment for two hours to

classify the rate of success. Most of the time, the success rate of IKS (94.7%) shows as best as compared of with AKAV1-MD5 (31.7%), with AKAV2-MD5 (31.4%).

TABLE IV. CALL SETUP (RESPONSE) TIME (*SEC*)

Protocols	Minimum	Maximum	Average
AKAV1-MD5	0.222	0.256	0.238
AKAV2-MD5	0.220	0.298	0.248
Proposed IKS	0.180	0.191	0.185

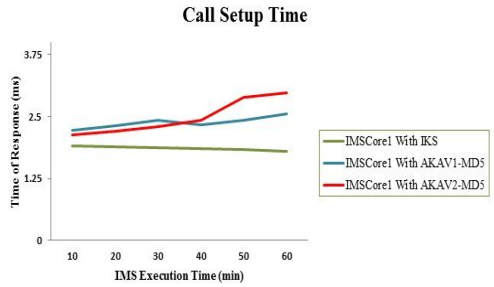

Figure 5. Call setup time

Fig. 5 illustrates call setup time of IMS environments. We have 12 PC's (6PC's are installed of UCTIMS and another 6PC's are installed of MonsterIMS) to inspect the response time of the calls (in seconds). We inspect the call active session for every five minutes. The experimental result is shown in Table IV wherein the IMS Core with IKS shows the most estimable results than the IMS Core with AKAV1-MD5 and AKAV2-MD5. Most of the time, IMS Core With IKS establishes the voice call to the clients at 1.8 ms whereas the IMS Core With AKAV1-MD5 establishes the voice call to the client at around 2.3 ms and IMSCore with AKAV2-MD5 sets up the call at around 2.4 ms. The mechanism of IKS not only has good call response time, but also, it has a better routing path to reduce the end-end delay.

V. CONCLUSION

In this research paper, a technique of IKS has been proposed for client schema interoperation, communication flexibility and storage security. The IKS has successfully patched with real time IMS Core to interoperate the client schema proficiently. The patching of ASI helps to retrench the key computation therefore it has reasonable call response time. It stabilizes the key validation between the clients therefore it has a good call success rate. By the improvement of the call success rate and interoperation success rate, we pronounce that the proposed technique of IKS could be able solve the issue of interoperation and flexibility.

Even though the tested multimedia client had not had any IBM based Codec, the audio channel allocation and bandwidth utilization was reasonably better than the other schema techniques. Thus, we conclude that the proposed formulation can patch with any real time based IMS environment to solve the challenging issues of any 3G based wireless communication standards.

ACKNOWLEDGMENT

The authors wish to thank TATA Consultancy Services (TCS) for Research Motivation and Financial Assistance.

REFERENCES

[1] 3GPP. [Online]. Available: http://www.3gpp.org/
[2] 3GPP Release 99, *3rd Generation Partnership Project - Technical Specifications and Technical Reports for a UTRAN-based 3GPP System*, TR 21.10, 1999.
[3] 3GPP Release 4, *3rd Generation Partnership Project - Technical Specifications and Technical Reports for a UTRAN-based 3GPP System and GERAN Features Content Functionally Frozen*, TR 41.101, 2001.
[4] 3GPP Release 5, *3rd Generation Partnership Project - Technical Specifications and Technical Reports for a UTRAN-based 3GPP system, and HSDPA*, TR 41.101, 2002.
[5] 3GPP Release 6, *3rd Generation Partnership Project - Technical Specifications and Technical Reports for a UTRAN-based 3GPP System Integrated Operation with Wireless LAN Networks, Adds HSUPA, MBMS, Enhancements to IMS Such as Push to Talk Over Cellular (PoC) and GAN*, TR 41.101, 2004.
[6] 3GPP Release 7, *3rd Generation Partnership Project - Technical Specifications and Technical Reports for a UTRAN-based 3GPP system Integrated Operation with Wireless LAN Networks on Decreasing Latency, Improvements to QoS and Real-Time Applications Such as VoIP*, TR 41.101, 2007.
[7] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnstone, J. Peterson, and R. Sparks, "SIP: Session initiation protocol," *IETF RFC3261*, 2002.
[8] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, and T. Haukka, "Security mechanism agreement for SIP sessions," *IETF Internet Draft*, 2002.
[9] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, and A. Luotonen, "HTTP authentication: Basic and digest access authentication," *IETF RFC2617*, 1999.
[10] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, and S. Ehlert, "Survey of security vulnerabilities in session initiation protocol," *IEEE Commun Surv Tutorials*, vol. 8, no. 3, pp. 68–81, 2006.
[11] M. Thomas *et al*., "SIP security requirements," *IETF Internet Draft*, (work in progress), November 2001.
[12] L. Veltri, S. Salsano, and D. Papalilo, "SIP security issues: The SIP authentication procedure and its processing load," *IEEE Netw*, vol. 16, no. 6, pp. 38–44, 2002.
[13] M. Handley *et al*., "SIP: Session Initiation protocol," *IETF Internet Draft*, *RFC 2543*, March 1999.
[14] C. C. Yang, R. C Wang, and W. T. Liu, "Secure authentication scheme for session initiation protocol," *Comput Secur*, vol. 24, pp. 381–386, 2005.
[15] M. Toorani and A. A. B. Shiraz, "A directly public verifiable signcryption scheme based on elliptic curves," in *Proc. 14th IEEE Symposium on Computers and Communications*, Tunisia, 2009, pp. 713–716.
[16] W. Diffie and M. Hellman, "New directions in cryptology," *IEEE Transaction on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976.
[17] A. Durlanik and I. Sogukpinar, "SIP authentication scheme using ECDH," *World Academy of Science Engineering and Technology*, vol. 8, pp. 350–353, 2005.
[18] Bellman and Bob, "Exploring IMS security mechanisms," *Business Communications Review*, January 2007.
[19] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, S. Ehlert, C. Lambrinoudakis, *et al*., "Survey of security vulnerabilities in

session initiation protocol," *IEEE Communications Surveys and Tutorials*, vol. 8, pp. 68–81, May 2006.
[20] M. Boucadair, P. Morand, I. Borges, and M. Tomsu, "Enhancing the serviceability of IMS-based multimedia services: Preventing core service failures," *International Journal of Internet Protocol Technology*, vol. 3, no. 4, pp. 224-233, 2008.
[21] M. T. Hunter, R. J. Clark, and F. S. Park, "Security issues with the IP multimedia subsystem (IMS)," in *Proc. ACM Workshop on Middleware for Next-Generation Converged Networks and Applications*, Article 9, New York, 2007.
[22] W.-S. Juang, C.-L. Lei, H.-T. Liaw, and W.-K. Nien, "Robust and efficient three-party user authentication and key agreement using bilinear pairings," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 2, pp. 763-772, 2010.
[23] H.-C. Hsiang, "A novel dynamic ID-based remote mutual authentication scheme," *International Journal of Innovative Computing, Information and Contro*l," vol. 6, no. 6, pp. 2407-2415, 2010.
[24] C. L. Lin and T. Hwang, "A password authentication scheme with secure password updating," *Comput Secur*, vol. 22, no. 1, pp. 68–72, 2003.
[25] M. Abdalla and D. Pointcheval, "Interactive dife-hellman assumptions with applications to password-based authentication," in *Proc. Financial Cryptography and Data Security-FC*, Dominica, 2005, pp. 341-56.
[26] M. Abdalla and D. Pointcheval, "Simple password-based encrypted key exchange protocols," in *Proc. Topics in Cryptology-CT-RSA*, USA, 2005, pp. 191-208.
[27] M. Bellare, D. Pointcheval, and P. Rogaway, " Authenticated key exchange secure against dictionary attacks," in *Proc. Advances in Cryptology Eurocrypt*, Belgium, 2000, pp. 139-155..
[28] S. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in *Proc. IEEE Computer Society Symposium on Research in Security Privacy*, USA, 2002, pp. 72-84.
[29] S. Bellovin and M. Merritt, "Augmented encrypted key exchange: password-based protocols secure against dictionary attacks and password file compromise," in *Proc. 1st ACM Conference on Computer and Communications Security*, November 1993, pp. 244-250.
[30] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password authenticated key exchange usinG dife-hellman," in *Proc. 19th International Conference on Theory and Application of Cryptographic Techniques*, Heidelberg, 2000, pp. 156-171.
[31] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "An efficient protocol for authenticated key agreement," *Designs, Codes and Cryptography*, vol. 28, no. 2, pp. 119-134, 2003.
[32] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, January 1987.
[33] V. Miller, "Use of elliptic curves in cryptography," in *Proc. Advances in Cryptology CRYPTO*, USA, 1985, pp. 417-426.
[34] X-Lite. [Online]. Available: http://www.counterpath.com/x-lite.html
[35] Zoiper. [Online]. Available: http://www.zoiper.com/download_list.php
[36] Open Source IMS Core Network. [Online]. Available: http://www.openim-score.org/.
[37] Ntop. [Online]. Available: http://www.ntop.org/get-started/download/
[38] M. Handley, SDP: Session Description Protocol, *IETF RFC 2327*, 1998.
[39] *3rd Generation Partnership Project*, TS 23.228: IP Multimedia Subsystem (IMS), 2006.
[40] K. D. Chang, C. Y. Chen, S. W. Hsu, H. C. Chao, and J. L. Chen, "Advanced path-migration mechanism for enhancing signaling efficiency in IP multimedia subsystem," *KSII Transactions On Internet and Information Systems*, vol. 6, no. 1, pp. 305-321, January 2012.
[41] H. M. Sun, B. Z. He, S. Y. Chang, and C. H. Cho, "Efficient authentication and key agreement procedure in IP multimedia subsystem for UMTS," *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 2, pp.1385-1396, February 2012.
[42] Wireshark, [Online]. Available: http://www.wireshark.org/

Rajappa Muthaiah obtained the degree of B.E (Electronic and Instrumentation) at Annamalai University, Chidambaram, India in 1989. He obtained the degree of M.E (Power Electronics and Industrial Drives) at Bharathidasan University, Thiruchupalli, INDIA in 1996. And then, he obtained the degree Ph.D. (Digital Image Compression) at SASTRA University, Thanjavur, INDIA in 2009.
He has had 3 years of experience in the industry sector and 21 years of experience in the academic sector. He worked as Lecturer for 12 years and Associate Professor for 2 years at SASTRA University, Thanjavur, INDIA. Since April 2013, he has been working as a Professor at the same University. He has so far had 28 International Journal papers and 5 International Conference papers. He is being a member of IE and AECE. His research interest includes Image Processing, VLSI and Speech Recognition.

Bakkiam David Deebak obtained the degree of B.Tech (Information Technology) at Anna University, Chennai, India in 2007. He obtained the degree of M.E (Embedded System and Computing) at RTM Nagpur University, Nagpur, INDIA in 2009. Since July 2011, he has pursued the degree of Ph.D. (Wireless Multimedia Communication Networking) at SASTRA University, Thanjavur, INDIA.
He has had 6 months of experience in the industry sector and 2.5 years of experience in the academic sector. He worked as Lecturer for 1.8 years at KITS-RANTEK, India and then he worked as Assistant Professor for 1 year at Sundharsan Engineering College, Pudukottai, INDIA. He has so far had 3 International Journal papers and 6 International Conference papers. He is an active member of IE. His research interest includes Computer Networks, Wireless Networks and Network Security, Multimedia Communication and Protocols.

Karuppusamy Thenmozhi obtained a Ph.D. degree from SASTRA University in 2008. Currently, he is working as Associate Dean in School of Electrical and Electronics Engineering at SASTRA University. Her research interest includes Networking and Wireless Communication.

Pitchai Iyer Swaminathan obtained Doctorate Degree in Electronics and Communication Engineering. Currently, he is working as Dean in School of Computing at SASTRA University. His research interest includes Embedded Systems, Software Engineering and Expert Systems.